US sanctions Chinese firm, hacker behind telecom and Treasury hacks

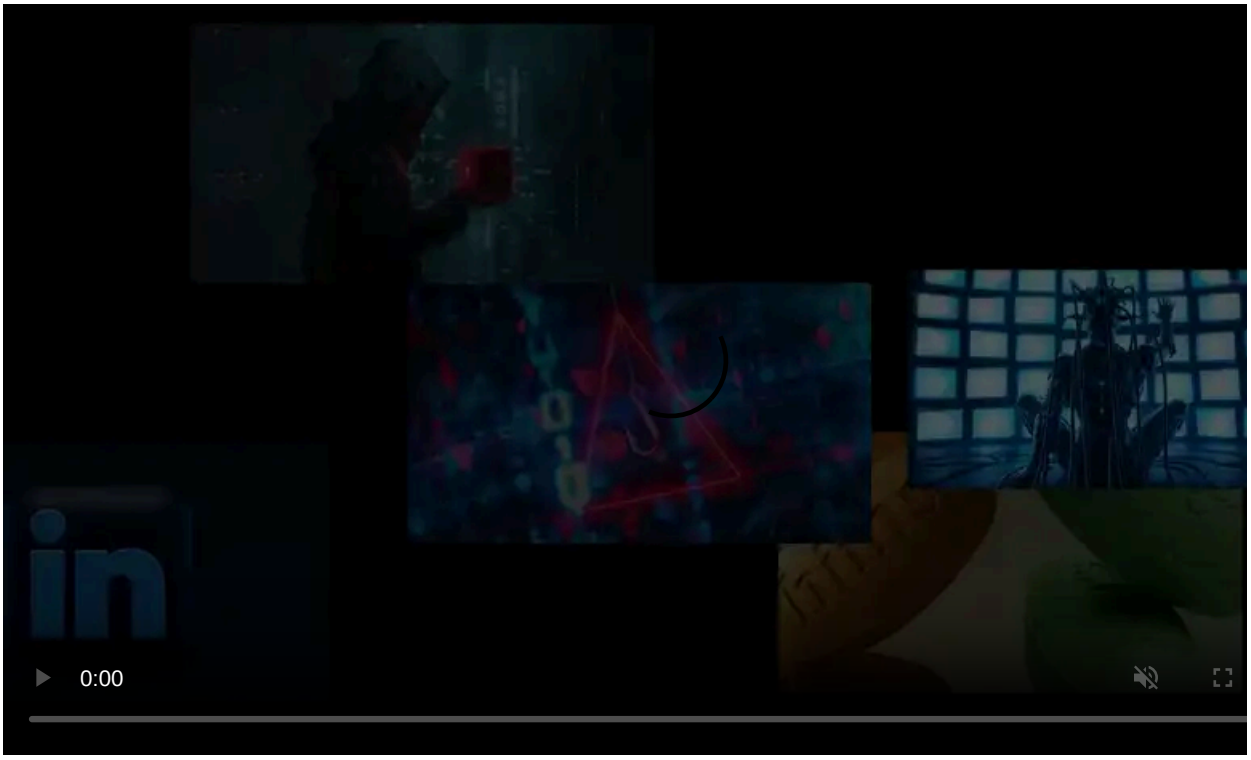
By Bill Toulas

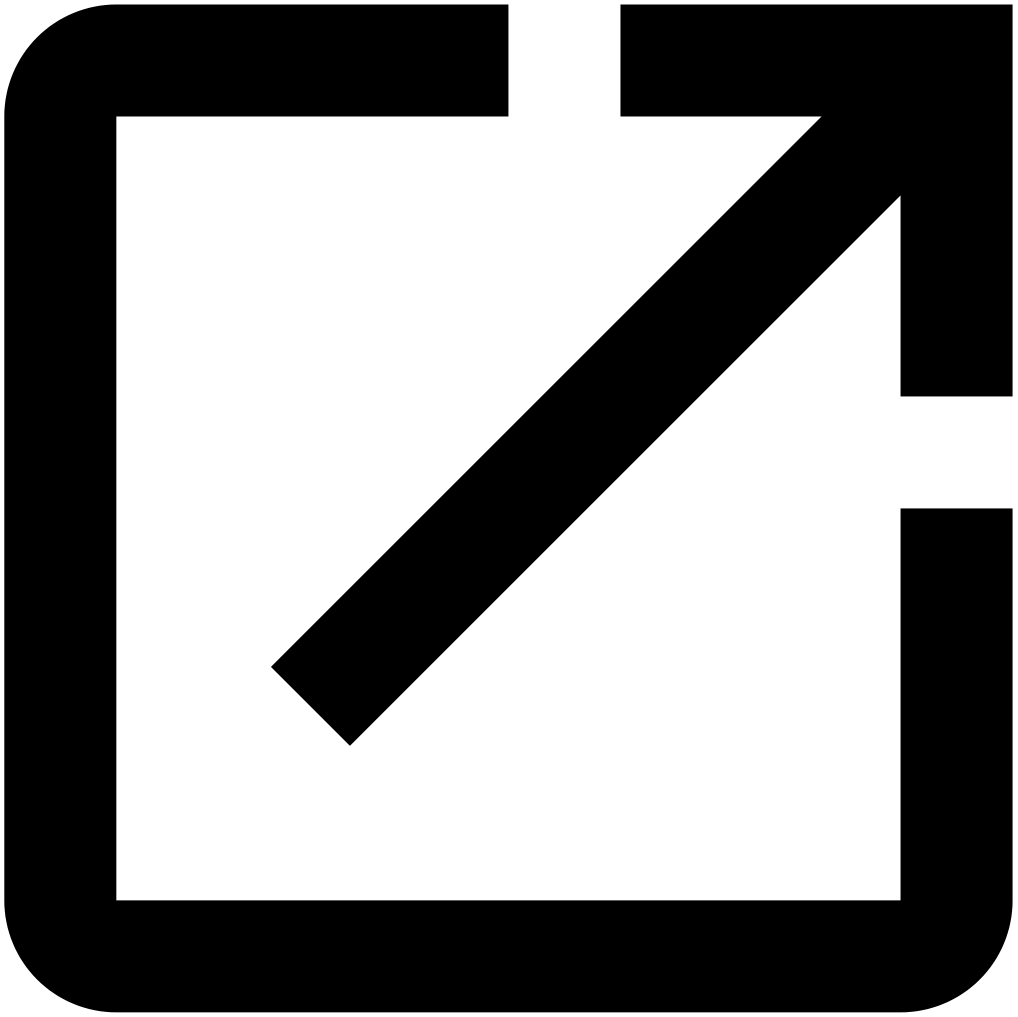
Published: 2025-01-17 · Archived: 2026-04-05 15:45:56 UTC

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned Yin Kecheng, a Shanghai-based hacker for his role in the recent Treasury breach and a company associated with the Salt Typhoon threat group.

"Yin Kecheng has been a cyber actor for over a decade and is affiliated with the People's Republic of China Ministry of State Security (MSS)," reads the Treasury's announcement.

"Yin Kecheng was associated with the recent compromise of the Department of the Treasury's Departmental Offices network," says the agency.


0:00



OFAC also announced sanctions against Sichuan Juxinhe Network Technology Co., a Chinese cybersecurity firm believed to be directly involved with the Salt Typhoon state hacker group.

Salt Typhoon was recently linked to several breaches on major U.S. telecommunications and internet service providers to spy on confidential communications of high-profile targets.

“Sichuan Juxinhe Network Technology Co., LTD. (Sichuan Juxinhe) had direct involvement in the exploitation of these U.S. telecommunication and internet service provider companies,” the U.S. Treasury explains, adding that “the MSS has maintained strong ties with multiple computer network exploitation companies, including Sichuan Juxinhe.”

The attack on the U.S. Treasury was disclosed to the public in late December 2024. The breach was possible after the hackers exploited a zero-day vulnerability in the remote support platform BeyondTrust.

The attack was attributed to Chinese state-backed hackers, who targeted the sanctions office specifically.

Last week, the Treasury announced that the operation was conducted by “Silk Typhoon” (a.k.a. Hafnium), a team of skilled cyberspies who target a broad range of organizations in the U.S., Japan, Australia, and Vietnam.

The sanctions imposed on Kecheng and the Chinese cybersecurity firm under Executive Order (E.O.) 13694 block all property and financial assets located in the United States or are in the possession of U.S. entities, including banks, businesses, and individuals.

Additionally, U.S. entities are prohibited from conducting any transactions with the sanctioned entities without OFAC's explicit authorization.

It’s worth noting that these sanctions come after OFAC sanctioned Beijing-based cybersecurity company Integrity Tech for its involvement in cyberattacks attributed to the Chinese state-sponsored Flax Typhoon hacking group.

U.S. Treasury's announcement reiterates that the U.S. Department of State offers, through its Rewards for Justice program, up to $10,000,000 for information leading to uncovering the identity of hackers who have targeted the U.S. government or critical infrastructure in the country.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
